3. MORE ON SUBGROUPS & CYCLIC GROUPS

Recall that we say a subset H of a group G is a **subgroup of** G if H is a group in its own right under the restriction of G's group operation. We write this

$$H \leqslant G.$$

There is a simple check – the *subgroup test* – for determining whether a subset is a subgroup.

Proposition 87 *(**Subgroup Test**) Let G be a group. Then a $H \subseteq G$ is a subgroup of G if and only if H is non-empty and whenever $x, y \in H$ then $x^{-1}y \in H$.*

Proof. $\Longrightarrow$ Suppose that $H \leqslant G$. Then $e \in H$ and so H is non-empty. Further for $x, y \in H$ we have $x^{-1}y \in H$ as H is closed under products and inverses.

$\Longleftarrow$ Suppose that the subgroup test applies. As $H \neq \varnothing$ then there is some $h \in H$ and so by the test $e = h^{-1}h \in H$. Further if $x, y \in H$ then by the test $x^{-1} = x^{-1}e \in H$ and $xy = (x^{-1})^{-1}y \in H$. Thus H is closed under products and inverses. Finally the associativity of the group operation on H is inherited from its associativity on G. ∎

Example 88 *The subgroups of S_3 are*

$$\{e\}, \qquad \{e, (12)\}, \qquad \{e, (13)\}, \qquad \{e, (23)\}, \qquad A_3, \qquad S_3.$$

Solution. The listed subgroups are certainly subgroups of S_3. To see that these are the only subgroups suppose that $H \leqslant S_3$. Certainly $e \in H$. If $|H| = 2$ then H must consist of e and a non-trivial self-inverse element. If $|H| = 3$ then it must be of the form $\{e, g, g^2\}$ where $g^3 = e$ and A_3 is the only such subgroup. If $|H| \geqslant 4$ then H must either (i) contain all three 2-cycles or (ii) a 2-cycle and a 3-cycle. As the product of two 2-cycles in S_3 is a 3-cycle, we see case (ii) in fact subsumes case (i). Also if H contains a 3-cycle then it contains its inverse. So, without any loss of generality we may assume this 2-cycle and 3-cycle to be (12) and (123). But then

$$(13) = (12)(123), \qquad (23) = (123)(12), \qquad (132) = (123)^2$$

and we see that $H = S_3$. ∎

Example 89 *The subgroups of D_8 are*

$$\begin{array}{llllll} \{e\}, & \{e, r^2\}, & \{e, s\}, & \{e, rs\}, & \{e, r^2 s\}, & \{e, r^3 s\}, \\ \{e, r, r^2, r^3\}, & \{e, r^2, s, r^2 s\}, & \{e, r^2, rs, r^3 s\}, & D_8. & & \end{array}$$

Solution. The listed subgroups are certainly subgroups of D_8. To see that these are the only subgroups suppose that $H \leqslant D_8$. Certainly $e \in H$. If $|H| = 2$ then H must consist of e and a non-trivial self-inverse element and the possibilities are listed above. If $|H| = 3$ then it must be of the form $\{e, g, g^2\}$ where $g^3 = e$ but there is no such $g \in D_8$. A subgroup of order 4 must

be of the form $\{e, g, g^2, g^3\}$ where $g^4 = e$ or $\{e, a, b, ab\}$ where $a^2 = b^2 = e$ and $ab = ba$. For the former, only $g = r$ or $g = r^3$ will do which both lead to the same subgroup $\{e, r, r^2, r^3\}$. For the latter we must have two reflections and a rotation; further the rotation must be r^2 if it is to commute with the reflections. So the only possibilities are $\{e, r^2, s, r^2s\}$ and $\{e, r^2, rs, r^3s\}$. If $|H| \geqslant 5$ then H must contain a rotation and a reflection; if the rotation is r or r^3 then it and the reflection will lead to all of D_8 but if there are three or more reflections then at least one must be in a diagonal and one in the vertical or horizontal and so their product is r or r^3. Hence $H = D_8$ is the only subgroup of order greater than 4. ■

Example 90 *The subgroups of $C_6 = \{e, g, g^2, g^3, g^4, g^5\}$ are*

$$\{e\}, \qquad \{e, g^3\}, \qquad \{e, g^2, g^4\}, \qquad C_6.$$

The only subgroups of C_5 are $\{e\}$ and C_5.

Solution. The only non-trivial self-inverse element in C_6 is g^3 and the non-trivial solutions of $x^3 = e$ are g^2, g^4. If $H \leqslant C_6$ and $|H| \geqslant 4$ then either $g \in H$ or $g^5 = g^{-1} \in H$ (both of which lead to $H = C_6$) or $\{e, g^2, g^3, g^4\} \subseteq H$ in which case $g^3 (g^2)^{-1} = g \in H$ in which case $H = C_6$ is the same conclusion.

If $H \leqslant C_5$ and $1 \in H$ then $H = C_5$ but if $g^2 \in H$ then $(g^2)^3 = g \in H$, and if $g^3 \in H$ then $(g^3)^{-1} = g^2 \in H$ and if $g^4 \in H$ then $(g^4)^{-1} = g \in H$. So $H = \{e\}$ or $H = C_5$. ■

Remark 91 *You may have noticed that in each of the previous examples, $|H|$ divides $|G|$ and this is indeed the case. This result is known as **Lagrange's Theorem** and we will prove in the next chapter.*

Proposition 92 *Let G be a group and H, K be subgroups of G. Then $H \cap K$ is a subgroup.*

Proof. This is left as Exercise Sheet 3, Question 2. ■

In fact, it is very easy to generalize Proposition 92 to show that if H_i (where $i \in I$) form a collection of subgroups of G then

$$\bigcap_{i \in I} H_i \leqslant G.$$

Thus we may make the following definition.

Definition 93 *Let G be a group and S a subset of G.*
*(i) The **subgroup generated by** S, written $\langle S \rangle$, is the smallest subgroup of G which contains S. (This is well-defined as G is a subgroup of G which contains S and $\langle S \rangle$ is then the intersection of all such subgroups.)*
(ii) If $g \in G$, then we write $\langle g \rangle$ rather than the more accurate but cumbersome $\langle \{g\} \rangle$.
*(iii) If $\langle S \rangle = G$ then the elements of S are said to be **generators** of G.*

Example 94 *Determine $\langle S \rangle$ in each of the following cases:*
(i) $G = \mathbb{Z}$, $S = \{12, 42\}$.
(ii) $G = S_4$, $S = \{(123), (12)(34)\}$.
(iii) $G = \mathbb{Q}^*$, $S = \{3, \frac{2}{3}\}$.

Solution. (i) Note that $6 = 42 - 3 \times 12$; hence $6 \in \langle S \rangle$ and $6\mathbb{Z} \subseteq \langle S \rangle$. But as $12 = 2 \times 6$ and $42 = 7 \times 6$ then $\langle S \rangle \subseteq 6\mathbb{Z}$. This $\langle S \rangle = 6\mathbb{Z}$.

(ii) As $(123) \in A_4$ and $(12)(34) \in A_4$ then certainly $\langle S \rangle \subseteq A_4$. If we write $\sigma = (123)$ and $\tau = (12)(34)$ then we see that the following are also in A_4.

$$\begin{array}{cccc} e, & \sigma = (123), & \tau\sigma\tau = (214), & (\tau\sigma\tau)^2 = (124), \\ \sigma^2\tau\sigma = (14)(23), & \sigma\tau\sigma^2 = (13)(24), & \tau = (12)(34), & \sigma^2 = (132), \\ \sigma\tau = (243), & (\sigma\tau)^2 = (234), & \tau\sigma = (134), & (\tau\sigma)^2 = (143). \end{array}$$

Hence $\langle S \rangle = A_4$.

(iii) We have $3 \in \langle S \rangle$ and so $3^m \in \langle S \rangle$ for all $m \in \mathbb{Z}$. Likewise $2 = \frac{2}{3} \times 3 \in \langle S \rangle$ so that $2^n \in \langle S \rangle$ for all $n \in \mathbb{Z}$. So $2^n 3^m \in \langle S \rangle$ for $m, n \in \mathbb{Z}$. But as these form a subgroup of $\mathbb{Q}^*$ (see the next example) we have

$$\langle S \rangle = \{2^n 3^m : m, n \in \mathbb{Z}\}.$$

■

Example 95 *Show that if G is abelian and $g, h \in G$ then*

$$\langle g, h \rangle = \{g^r h^s : r, s \in \mathbb{Z}\}.$$

Solution. Certainly $\{g^r h^s : r, s \in \mathbb{Z}\} \subseteq \langle g, h \rangle$. However, when G is abelian (or indeed if just $gh = hg$), then $\{g^r h^s : r, s \in \mathbb{Z}\}$ is a subgroup as follows:

(i) $e = g^0 h^0 \in \{g^r h^s : r, s \in \mathbb{Z}\}$;

(ii) $\left(g^k h^l\right)\left(g^K h^L\right) = g^{k+K} h^{l+L} \in \{g^r h^s : r, s \in \mathbb{Z}\}$;

(iii) $\left(g^k h^l\right)^{-1} = h^{-l} g^{-k} = g^{-k} h^{-l} \in \{g^r h^s : r, s \in \mathbb{Z}\}$. ■

Remark 96 *In several of the results that follow, notably Proposition 97 and Theorem 102 we make use of the following fact, known as the* ***division algorithm****, which we will take as self-evident.*

- *Let a, b be integers with $b > 0$. Then there exist unique integers q, r such that $a = qb + r$ and $0 \leqslant r < b$.*

Proposition 97 *Let G be a group and $g \in G$. Then*

(a) $\langle g \rangle = \left\{g^k : k \in \mathbb{Z}\right\}$.

(b) If $\mathrm{o}(g)$ is finite then $\langle g \rangle = \left\{e, g, g^2, \ldots, g^{\mathrm{o}(g)-1}\right\}$.

Proof. (a) As $g^k \in \langle g \rangle$ for any integer k, so it only remains to show that $H = \left\{g^k : k \in \mathbb{Z}\right\}$ is indeed a subgroup. Using the subgroup test we note $g^0 = e \in H$ and that if $g^k, g^l \in H$ then

$$(g^k)^{-1} g^l = g^{-k} g^l = g^{l-k} \in H.$$

Hence $\langle g \rangle = H$.

(b) It is again clear that $\left\{e, g, g^2, \ldots, g^{\mathrm{o}(g)-1}\right\} \subseteq \langle g \rangle$. Also for any $k \in \mathbb{Z}$ there exist $q, r \in \mathbb{Z}$ such that $k = q\mathrm{o}(g) + r$ where $0 \leqslant r < \mathrm{o}(g)$. Then

$$g^k = g^{q\mathrm{o}(g)+r} = \left(g^{\mathrm{o}(g)}\right)^q g^r = e^q g^r = g^r \in \left\{e, g, g^2, \ldots, g^{\mathrm{o}(g)-1}\right\}.$$

■

Remark 98 *Recall that we say that a group G is* **cyclic** *if there exists $g \in G$ such that $G = \langle g \rangle$. Note also that a cyclic group is necessarily abelian.*

Remark 99 *Note that in a finite group G, then g is a generator if and only if $\mathrm{o}(g) = |G|$.*

Example 100 *(i) C_6 is cyclic with generators g and g^5.*

(iii) C_5 is cyclic with generators g, g^2, g^3, g^4.

(iv) $C_2 \times C_2$ is not cyclic as the elements have orders $1, 2, 2, 2$.

(v) $C_2 \times C_3$ is cyclic. If $C_2 = \{e, g\}$ and $C_3 = \{e, h, h^2\}$ then (g, h) and (g, h^2) are both generators of $C_2 \times C_3$ as they have order 6 (check!).

(vi) $\mathbb{Q}$ is not cyclic: clearly $\langle 0 \rangle \neq \mathbb{Q}$ and if $q \neq 0$ then $\frac{1}{2}q \notin \langle q \rangle = q\mathbb{Z}$. By the same reasoning we see that $\mathbb{Q}$ cannot be generated by finitely many elements.

Theorem 101 *Let G be a cyclic group.*

(a) If $|G| = n$ is finite, then G is isomorphic to C_n.

(b) If $|G|$ is infinite, then G is isomorphic to $\mathbb{Z}$.

Proof. (a) Let g be a generator of G. Then

$$G = \langle g \rangle = \left\{e, g, g^2, \ldots, g^{n-1}\right\}$$

by Proposition 97 (b) and multiplication in G is as given in Example 34 as $g^n = e$.

(b) If g is a generator of G with infinite order, then we can define a map $\phi : G \to \mathbb{Z}$ by $\phi(g^r) = r$ which is an isomorphism. ■

Theorem 102 *Let G be a cyclic group and $H \leqslant G$. Then H is cyclic.*

Proof. Let $G = \langle g \rangle$. If $H = \{e\}$ then $H = \langle e \rangle$ and we are done. Otherwise, we define

$$n = \min\left\{k > 0 : g^k \in H\right\}.$$

To show that n is well-defined, note that $g^k \in H \neq \{e\}$ for some $k \neq 0$. As H is a subgroup then $g^{-k} = \left(g^k\right)^{-1} \in H$ also. As one of $\pm k$ is positive, n is well-defined. We will show that

$$H = \langle g^n \rangle.$$

As $g^n \in H$ then $\langle g^n \rangle \subseteq H$. Conversely say that $g^a \in H$. Then, by the division algorithm, there exist $q, r \in \mathbb{Z}$ such that $a = qn + r$ where $0 \leqslant r < n$. But then

$$g^r = g^{a-qn} = g^a \left(g^n\right)^{-q} \in H$$

as $g^a \in H$ and $g^n \in H$. By the minimality of n then $r = 0$ and $g^a = (g^n)^q \in \langle g^n \rangle$. ■

Corollary 103 *The subgroups of $\mathbb{Z}$ are each of the form $m\mathbb{Z}$ where $m \in \mathbb{Z}$.*

Proposition 104 *Let m, n be non-zero integers. By Theorem 102 we have*

$$\langle m, n\rangle = \langle h\rangle \qquad \langle m\rangle \cap \langle n\rangle = \langle l\rangle$$

for some $h, l > 0$. Then h has the following properties:
(a) $h|m$ and $h|n$;
(b) if $x|m$ and $x|n$ then $x|h$;
(c) there exist $u, v \in \mathbb{Z}$ such that $um + vn = h$. ***(Bézout's Lemma)***
and l has the following properties:
(d) $m|l$ and $n|l$;
(e) if $m|x$ and $n|x$ then $l|x$.

Proof. Properties of h:
(a) As $m = 1m + 0n \in \langle m, n\rangle = \langle h\rangle$ then $h|m$. Similarly $h|n$.
(c) This follows from Example 95.
(b) Say $x|m$ and $x|n$. Then by Bézout's Lemma $x|um + vn$ and so $x|h$.
Properties of l:
(d) As $l \in \langle m\rangle$ then $m|l$. Similarly $n|l$.
(e) If $m|x$ then $x \in \langle m\rangle$. Likewise $x \in \langle n\rangle$. So $x \in \langle m\rangle \cap \langle n\rangle = \langle l\rangle$ and $l|x$. ■

Definition 105 *We define h, as defined in the previous Proposition, to be the* ***highest common factor*** *or* ***hcf*** *of m and n.*

We define l as defined in the previous Proposition, to be the ***least common multiple*** *or* ***lcm*** *of m and n.*

Theorem 106 ***(Chinese Remainder Theorem)*** *Let m and n be coprime natural numbers. Then C_{mn} is isomorphic to $C_m \times C_n$.*

Specifically if g is a generator of C_m and h is a generator of C_n then (g, h) generates $C_m \times C_n$.

Proof. Certainly

$$(g, h)^{mn} = \left((g^m)^n, (h^n)^m\right) = (e^n, e^m) = (e, e)$$

so that the order of (g, h) divides mn. But on the other hand $g^k = e$ if and only if $m|k$ and $h^k = e$ if and only if $n|k$. So

$$(g, h)^k = \left(g^k, h^k\right) = (e, e)$$

if and only if $m|k$ and $n|k$. As m, n are coprime then, by Bezout's Lemma, there exist u, v such that $um + vn = 1$. As $n|k$ then $mn|mk$ and as $m|k$ then $mn|nk$. So

$$mn \mid (umk + vnk) = k.$$

Hence the order of (g, h) is mn which equals $|C_m \times C_n|$. ■